A New Fast Algorithm for Computing a Complex Number — Theoretic Transforms

I. S. Reed and K. Y. Liu
University of Southern California

T. K. Truong
TDA Engineering Office

A high-radix FFT algorithm for computing transforms over $GF(q^2)$, where q is a Mersenne prime, is developed to implement fast circular convolutions. This new algorithm requires substantially fewer multiplications than the conventional FFT.

I. Introduction

Several authors (Refs. 1 through 3) have proposed the use of the fast Fourier transform (FFT) over finite fields or rings. Such transforms can be used to compute circular convolutions of real or complex integer sequences without round-off error (Refs. 4 through 11).

Recently, Winograd (Ref. 12) developed a new class of algorithms for computing the conventional discrete Fourier transform (DFT). This algorithm requires substantially fewer multiplications than the best FFT algorithm previously known.

Reed and Truong (Ref. 5) extended the integer transforms of Rader by defining a complex number-theoretic transform (CNT) over the Galois field $GF(q^2)$, where $q = 2^p - 1$ is a Mersenne prime. An FFT algorithm of length $d = 2^k$, where $1 \leqslant k \leqslant p + 1$, can be carried out in $GF(q^2)$ with $d \log_2 d$ multiplications. In this paper a mixed high-radix transform of $GF(q^2)$ is developed that requires only dm multiplications where m is a fractional number, depending on the factors of d, where d is an integer of form $2^k \cdot p (0 \leqslant k \leqslant p + 1)$. This algorithm for $GF(q^2)$ appears comparable in speed with that given by S. Winograd.

II. Transforms Over $GF(q^2)$

Let $GF(q^2)$ be a Galios field, where q is a Mersenne prime, and let the integer $d | q^2 - 1$. Also let the element $\gamma \epsilon GF(q^2)$ generate the cyclic subgroup of d elements $G_d = (\gamma, \gamma^2, \cdots,$

γ^{d-1}, 1) in the multiplicative group of $GF(q^2)$. Then a transform over this subgroup G_d can be defined by the following (Ref. 5):

$$A(f) = \sum_{t=0}^{d-1} a(t)\,\gamma^{ft} \qquad \text{for } 0 \leqslant f \leqslant d-1 \qquad (1)$$

where

$$a(t) \epsilon GF(q^2) \qquad \text{for } 0 \leqslant t \leqslant d-1$$

By Fermat's theorem $2^{p-1} \equiv 1 \bmod p$. Hence $p | 2^{p-1} - 1$. Thus, $t = 2^{p+1}(2^{p-1} - 1)$ has the factor $d = 2^{p+1} \cdot p$. A mixed-radix FFT algorithm will be developed now to calculate transforms of $d = 2^k \cdot p$ points, where $0 \leqslant k \leqslant p+1$.

To perform the transform over $GF(q^2)$, where $d | 2^{p+1} \cdot p$, it is necessary to find primitive elements in the d-element cyclic subgroup G_d in $GF(q^2)$. To do this, let α be a primitive element of $GF(q^2)$. Using a computer program, one can choose an element $\alpha = a + \hat{i}b$, where $a \neq 0$ and $b \neq 0$, such that

$$\alpha^{2^{p+1}(2^{p-1}-1)/2} \equiv -1 \bmod q \qquad (2)$$

If $\alpha = a + \hat{i}b$ satisfies Eq. (2), then, by Theorem 1 of Ref. 5, $\alpha = a + \hat{i}b$ is an element of order $2^{p+1}(2^{p-1} - 1)$ in $GF(q^2)$. If $d = p \cdot 2^k$, where $1 \leqslant k \leqslant p+1$, then the generator of G_d, a multiplicative subgroup of order d, is evidently

$$\gamma = 2^{2^{p-1-k}(2^{p-1}-1)/p}$$

Also, γ^j is a primitive element in G_d for $j = 1, 3, 5, \cdots, d-1$.

Brigham (Ref. 13) shows that a mixed-radix transform of length $d = r_1 r_2 \cdots r_n$, where r_i are the n radices, requires $d(r_1 + r_2 + \cdots + r_n)$ complex additions and $d(r_1 + r_2 + \cdots + r_n)$ complex multiplications to perform a conventional mixed-radix FFT. To develop a similar mixed-radix FFT over $GF(q^2)$, it is desirable that multiplications, involving the r_i^{th} roots of unity for $i = 1, 2, \cdots, n$ in $GF(q^2)$, be accomplished by circular shifts. As we shall see, this is made possible if one chooses $d = r_1 r_2 \cdots r_n = 2^k \cdot p$, where $r_i = 2$ or 4 or 8 for $i = 1, 2, \cdots, n-1$ and $r_n = 8p$, where $0 \leqslant k \leqslant p+1$. It will next be shown that each r_i^{th} root of unity is a power of 2 modulo q for $i = 1, 2, \cdots, n$.

To see this, suppose γ is a generator of the multiplicative subgroup G_d of order d, where $d = 2^k \cdot p$ for $0 \leqslant k \leqslant p+1$. Then by Theorem 1 of Ref. 5, γ satisfies

$$\gamma^{d/2} \equiv -1 \bmod q \qquad (3)$$

But also,

$$(1 + \hat{i})^{4p} \equiv (-4)^p \equiv -1 \bmod q \qquad (4)$$

where q is the Mersenne prime $2^p - 1$ so that again by Theorem 1 of Ref. 5 $(1 + \hat{i})$ is an element of order $8p$. This result has also been given in Ref. 7. Thus, combining Eqs. (3) and (4), a generator γ of G_d satisfies

$$\gamma^{d/8p} \equiv (1 + \hat{i}) \bmod q \qquad (5)$$

By Eq. (5), a computer program can be used to find primitive element γ of G_d that satisfies Eqs. (3) and (5). Note that the powers of $\gamma^{d/8p}$ are powers of 2 modulo q, i.e., $\gamma^{d/4p} \equiv 2 \bmod q$, $\gamma^{d/2p} \equiv 2^2 \bmod q$, $\gamma^{d/p} \equiv 2^4 \bmod q$, etc.

In $GF(q^2)$, the equation $X^2 \equiv -1 \bmod q$ has the unique solutions $X \equiv \pm \hat{i} \bmod q$. Hence, $\gamma^{d/4} \equiv \hat{i}$ or $-\hat{i} \bmod q$. The powers of $\gamma^{d/4}$ are thus $\hat{i}$, $-\hat{i}$, 1, or -1.

The following theorem given in Ref. 14 is stated now without proof. It is useful for finding the eighth roots of unity in $GF(q^2)$.

Theorem 1. If $q = 2^p - 1$ is a mersenne prime, then the only solutions of $X^2 \equiv \pm\hat{i} \bmod q$ over $GF(q^2)$ are

$$X \equiv \pm 2^{(p-1)/2}(1 \pm \hat{i}) \bmod q$$

By Theorem 1, $(\gamma)^{d/8}$ is one of the forms $\pm 2^{(p-1)/2}(1 \pm \hat{i}) \bmod q$.

If one combines the results of the above three paragraphs, one has shown that complex multiplications by γ^{d/r_i} or its powers for $r_i = 2, 4, 8, 8p$ can be accomplished simply by circular shifts instead of multiplications. Hence, if one applies a mixed-radix FFT algorithm (Ref. 13) to a transform over $GF(q^2)$, the set of r_i-point DFT's can be evaluated without complex integer multiplications before referencing by the so-called twiddle factors. As a consequence, the maximum number of modulo $-q$ complex integer multiplications by γ^j $(j = 0, 1, 2, \cdots, d-1)$ needed for an FFT over $GF(q^2)$ is

$d(n-1)$ where $d = 2^k p$, n is the number of FFT stages, and $0 \leq k \leq p+1$. Consider now a simple example: Let

$$q = 2^3 - 1 \; ; d = r_1 r_2 = (2^3 p) \cdot 2 = 24 \times 2, \quad p = 3$$

A mixed-radix, decimation-in-frequency, twiddle factor, FFT algorithm over $GF(7^2)$ is described as follows for this example.

Let f and t in Eq. (1) be expressed in two ways as:

$$f = f_1 \cdot 24 + f_0 \equiv (f_1 f_0) \tag{6}$$

$$t = t_1 \cdot 2 + t_0 \equiv (t_1 t_0) \tag{7}$$

where

$$0 \leq f_1 \leq 1 \qquad 0 \leq f_0 \leq 23$$

$$0 \leq t_1 \leq 23 \qquad 0 \leq t_0 \leq 1$$

Substituting Eqs. (6) and (7) into Eq. (1) yields

$$A(f_1 f_0) = \sum_{t_0=0}^{r_2-1} \sum_{t_1=0}^{r_1-1} a(t_1 t_0) \gamma^{(f_1 \cdot 24 + f_0)(t_1 \cdot 2 + t_0)}$$

The mixed-radix FFT algorithm over $GF(7^2)$ for $d = 48$ points is composed of the following two successive stages of computation:

Stage 1:

$$A^{(1)}(f_0 t_1) = \left[\sum_{t_1=0}^{23} a(t_1 t_0) \gamma^{f_0 t_1 \cdot 2} \right] \gamma^{f_0 t_0} \tag{8}$$

Stage 2:

$$A^{(2)}(f_1 t_0) = \left[\sum_{t_0=0}^{1} A^{(1)}(f_0 t_1) \gamma^{f_1 t_0 \cdot 24} \right] \tag{9}$$

Since $(4 + \hat{i})^{24} \equiv -1 \bmod 7$, $\gamma = 4 + \hat{i}$ is a primitive element in $GF(7^2)$. By Eq. (5), this choice of γ yields $\gamma^2 \equiv (1 + \hat{i}) \bmod 7$. Hence, using this and the fact that $\gamma^{48} \equiv 1 \bmod 7$ and $\gamma^{24} \equiv -1 \bmod 7$, it is clear that the term $\gamma^{f_0 t_1 \cdot 2}$ in Eq. (8) can assume only the values ± 1 or plus or minus a power of $(1 + \hat{i})$.

Since multiplications involving ± 1 do not involve a multiplication, and since multiplications involving powers of $(1 + \hat{i})$ mod 7 can be achieved by circular shifts, the 24-point discrete Fourier transform in the brackets of Eq. (8) can be evaluated without a multiplier unit. The results of Eq. (8) are referenced now by multiplying the twiddle factor $\gamma^{f_0 t_0}$. This requires a total of 12 complex integer multiplications modulo 7 for evaluating Eq. (8). Since $\gamma^{24} \equiv -1 \bmod 7$, by an argument similar to that used in Eq. (8), it is clear that Eq. (9) can also be evaluated without multiplications.

The number of complex integer multiplications used to perform a mixed-radix FFT over $GF(q^2)$ of $d = r_1 r_2$ points, where $r_1 = 2^3 p$, $r_2 = 2$ or 4 or 8, and $q = 2^{31} - 1$, is given in Table 1. The present algorithm, Winograd's new algorithm (Ref. 12) and the standard FFT (Ref. 15) are compared in Table 1 by giving the number of real multiplications needed to perform these algorithms. The results for Winograd's algorithm were obtained from Ref. 11, Table 2. In Table 1, one can see that the transforms over $GF(q^2)$ of $d = 31$, 62, 124, 248 points can be evaluated without multiplications. For $d > 248$, the transforms over $GF(q^2)$ appear comparable in speed with that given by Winograd (Ref. 12).

Acknowledgment

The authors wish to thank the members of the Advanced Engineering Group in the Deep Space Network of the Jet Propulsion Laboratory for their early support, suggestions, and encouragement of the research that led to this paper. Special thanks are due to Dr. B. Benjauthrit for his attentive review of the paper.

References

1. J. M. Pollard, "The Fast Fourier Transform in a Finite Field," *Math. Comput.*, Vol. 25, No. 114, April, 1971.
2. A. Schonhage, and V. Strassen, "Schnelle Multiplikation Grosser Zahlem," *Computing 7*, 1971, pp. 281-292.
3. C. M. Rader, "Discrete Convolution via Mersenne Transforms," *IEEE Trans. on Computers*, Vol. C-21, No. 12, December, 1972.
4. R. C. Agarwal and C. S. Burrus, "Number Theoretic Transforms to Implement Fast Digital Convolution," *Proceedings of the IEEE*, Vol. 63, No. 4 April, 1975.
5. I. S. Reed and T. K. Truong, "The Use of Finite Fields to Compute Convolutions," *IEEE Trans. Inf. Theory*, Vol. IT-21, No. 2, March 1975, pp. 208-212.
6. I. S. Reed and T. K. Truong, "Complex Integer Convolutions Over a Direct Sum of Galois Fields," *IEEE Trans. Info. Theory*, Vol. IT-21, November 1975.
7. E. Vegh and L. M. Leibow, "Fast Complex Convolution in Finite Rings," *IEEE Trans. on Acoustics, Speed, and Signal Processing*, Vol. Assp-24, No. 4, August 1976, pp. 343-344.
8. S. W. Golomb, I. S. Reed, and T. K. Truong, "Integer Convolutions over the Finite Field $GF(3 \cdot 2^n + 1)$," to be published in *SIAM Journal on Applied Mathematics*, March 1977.
9. I. S. Reed and T. K. Truong, "Convolutionals Over Residue Classes of Quadratic Integers," *IEEE Trans. Inf. Theory*, July 1976.
10. J. M. Pollard, "Implementation of Number Theoretic Transforms," *Electron Lett.*, 1976, Vol. 12, pp. 378-379.
11. K. Y. Liu, I. S. Reed, and T. K. Truong, "Fast Number Theoretic Transforms for Digital Filtering," *Electron Lett.*, Vol. 12, No. 24, pp. 644-646, 25 November 1976.
12. S. Winograd, "On Computing the Discrete Fourier Transform," *Proc. Nat. Acad. Math. U.S.A.*, Vol. 73, No. 4, pp. 1005-1006, April 1976.
13. E. O. Brigham, *The Fast Fourier Transform*, Prentice-Hall, Inc., 1974.
14. H. Murakami and I. S. Reed, "Recursive Realization of Finite Impulse Filters Using Finite Field Arithmetic," to be published in *IEEE Trans. Inf. Theory*, March 1977.
15. J. W. Cooley and J. W. Tukey, "An Algorithm for the Machine Calculation of Complex Fourier-Series," *Math of Comp., 19*, pp. 297-301. 1965.

Table 1. The complexity of the transform over $GF(q^2)$, where $q = 2^{31} - 1$

d	No. of real integer multiplications of transform over $GF(q^2)$ of complex data	No. of real multiplications of Winograd's new algorithm for complex data	$2d\log_2 d$ real multiplications for conventional FFT (d is a power of 2)
31	0		
30		72	295
62	0		
60		144	709
124	0		
120		288	1658
248	0		
240		648	3796
496	496		
504		1872	9050
992	1984		
1008		4212	20115
1984	5456		
2520		11232	56949